**8-2 Journal: Portfolio Reflection**

Reflecting on this course, it’s clear that early adoption of secure coding standards, assessing risks and costs, implementing zero trust, and having strong security policies are crucial for building secure systems.

Adopting secure coding standards from the start prevents vulnerabilities and creates robust applications. Integrating security practices early is essential to avoid common issues like SQL injection and cross-site scripting. Evaluating risks and understanding the cost-benefit of mitigation is vital. By identifying threats and vulnerabilities, we can prioritize fixes based on their potential impact and cost. Balancing the cost of security measures with the potential damage of breaches is key.

Zero trust means continuously verifying every access request, assuming no one is inherently safe. This requires strict access controls, multi-factor authentication, and constant monitoring to reduce unauthorized access and breaches. Educating users and developers is essential for effective implementation.

Strong security policies ensure consistent practices and clear roles in protecting information. Policies should cover data protection, access control, incident response, and regular training. Involving various departments and regular reviews helps keep policies effective and up to date.

A proactive approach to security—adopting secure coding standards early, assessing risks and costs, implementing zero trust, and enforcing strong security policies—creates a solid foundation for safeguarding systems. These practices protect against current and future cybersecurity threats, and I am now better equipped to contribute to secure and resilient systems.